Journal of Emerging Trends and Novel Research
JETNR.ORG | ISSN : 2984-9276
An International Open Access, Peer-reviewed, Refereed Journal

The Art of Hacking

The complete guide to black hat hacking by an industrial expert hacker who works with law enforcement.

Priyank Dinesh Gada - IlluminatiOn Production House - Bharatiya Shesha University - Mumbai, India

Abstract: The invention of computers and smartphones is one of the biggest achievements in the world of technology. Smartphones today can do almost everything: faster networking, file management, and other powerful applications. Huge markets are adopting smartphones due to their flexibility and so are hackers. All though smartphones are of great importance, they have a number of setbacks as well. We are going to take a look at how credit card hacking works, how smartphones can be hacked, How SIM Swapping works, and other techniques witha practical approach. How to change IMEI number and other Black Hat Hacking techniques used by Hackers

Keywords- Ethical Hacking, Cyber Security, Network Security, Banking, CISCO, Hacking.

I. Introduction

Smartphone security is a major and important topic to be discussed today. About 40 % of the population is using the internet and so is vulnerable to various internet-based attacks. We can stop a person who physically attacks us but stopping a person in a virtual world is very difficult. A normal person using the internet daily for 1 hour is on average vulnerable to at least 3 attacks wherein the attacker can damage the victim.

II. CRACK Android PIN

Android PIN can be cracked easily. The Android OS is a Linux based software and thus it actually compares your pattern and pin with a file. There are various methods of cracking PIN and Pattern in android. You can delete the gesture.key file and password.key file in system folder inside the data directory of your android. You can also crack PIN with bruteforce attack. Priyank Gada has developed a custom board with a rubber ducky that can try combinations of password from 0000 to 9999 and unlock PIN. There are two major methods to crack android PIN and patterns.

A. Cracking Android PIN with Arduino and Rubber Ducky

A USB rubber ducky with an Arduino board can be used to create a brute-force attack. A brute-force attack means to try a combination of PINs from 0000 to 9999 and these PINs can be cracked and the board can also go to sleep for a timeframe that basically bypasses traditional method of cooldown for 5 minutes after 5 wrong PIN attempts that android has. This method does not require anything and has been tested by Priyank Gada on Motorola, Google Pixel and OnePlus devices. POC can be found on Priyank Gada's Instagram Profile.

The device is cheap and is worth 10$ and can be purchased from amazon and configured. An OTG cable can be attached. Hence it is always adviced to disable Developer options on your device and block your charging port and avoid giving your device to someone physically.

B. Cracking Android PIN and Pattern with Custom Recovery and Aroma File Manager

Android is a linux based operating system and hence it is file and process based. A basic mechanism is used i.e. comparing the PIN pattern entered by the user with the already set pattern. The saved pattern and PIN is hashed and saved in /DATA/SYSTEM/Gesture.key and /DATA/System/Password.key file. It is nearly impossible to recover the password but another method can be used to crack patterns. You can delete the file or replace it with a file with same device but a different pattern to change or use a new pattern. If the file is deleted, traditional phones like vivo and oppo can be unlocked without patterns but for phones like OnePlus and google Pixel, a same device ID file can be used to replace the older thus changing the pattern

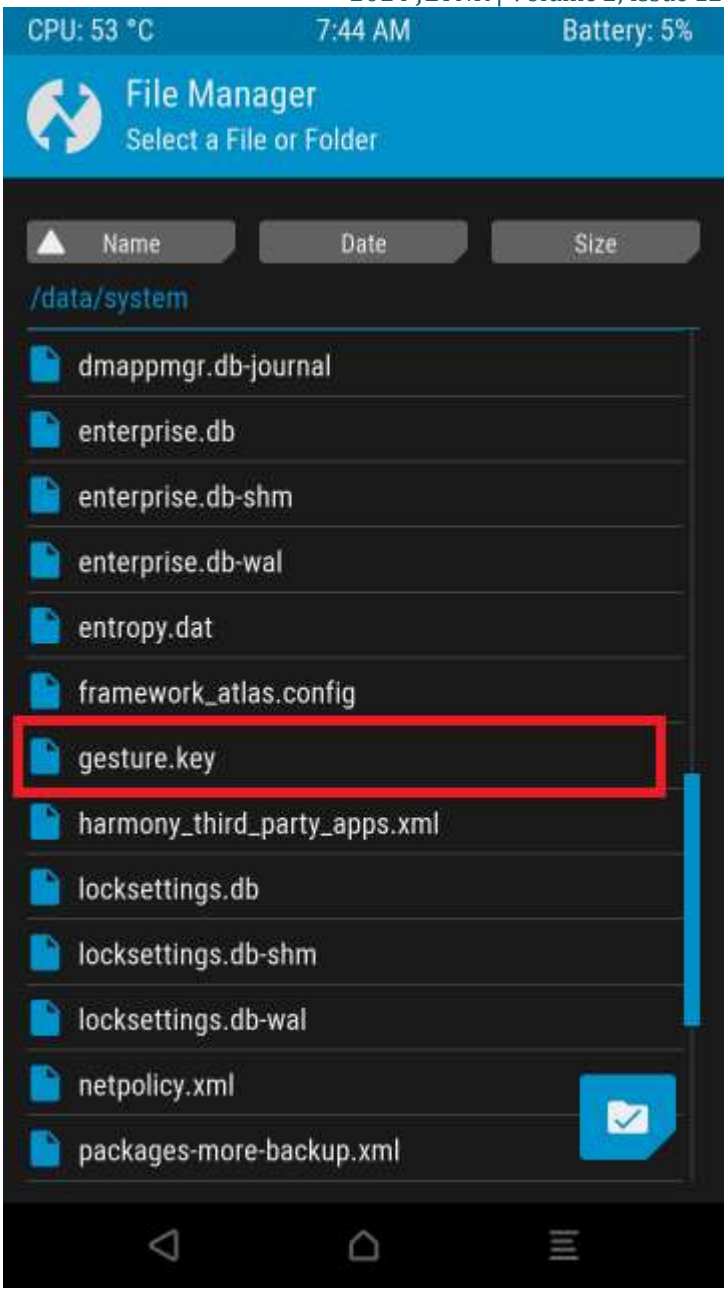


Image taken from an actual demonstration of TWRP recovery and Gesture.key file

Root your android device, install custom recovery, that can be a CWM recovery or TWRP or any other recovery whichever is supported by the device. Install file manager to delete or replace the Gesture.key file or password.key file. Samsung phones support TWRP recovery that already has a file manager. You can flash any recovery and later use AROMA file manager to browse file and delete or replace file.

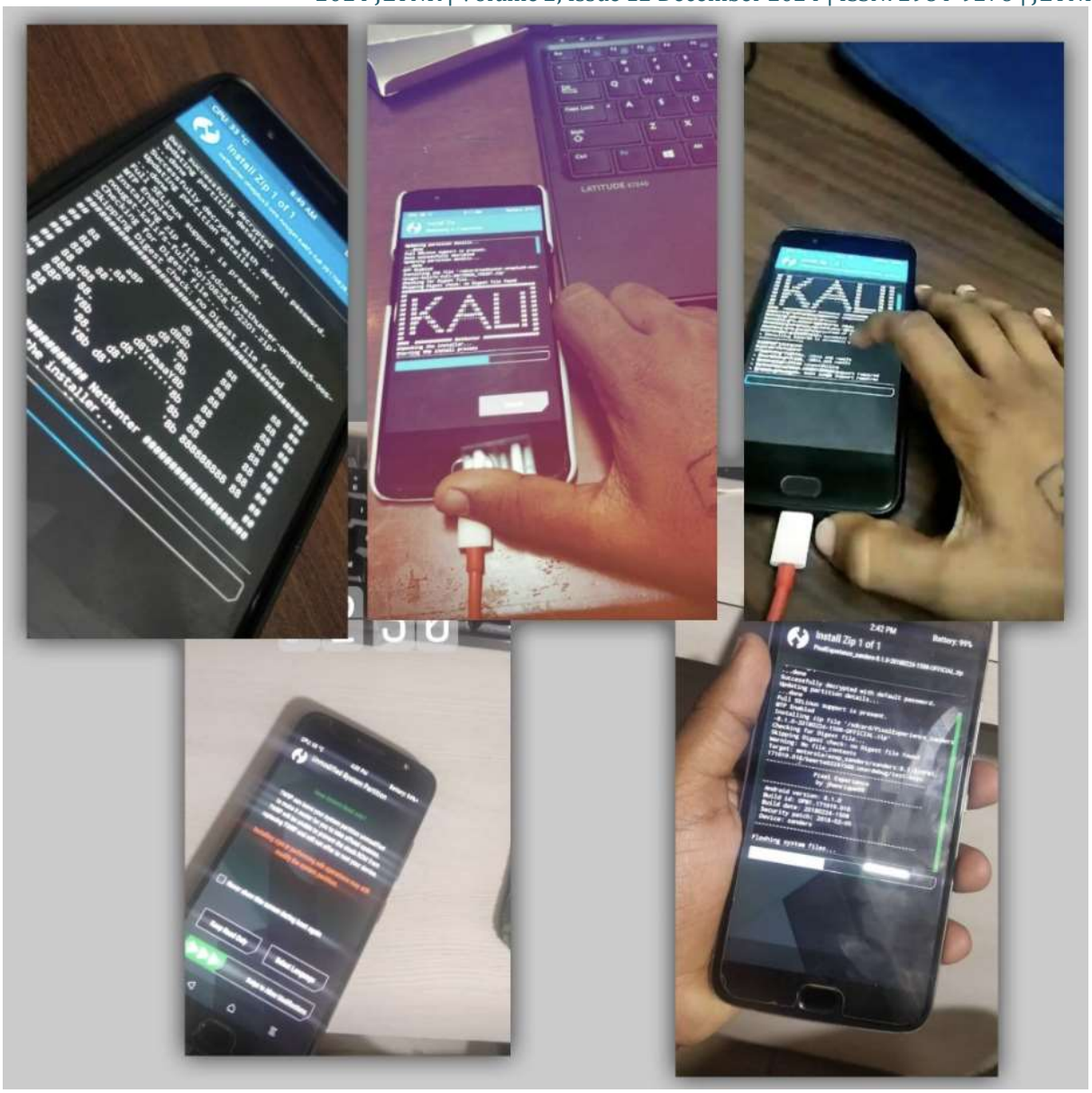


Image taken from actual demonstration of Android PIN Pattern hacking by Priyank Gada

III. Credit Card Hacking with Skimmer

Skimming in cybersecurity is a technique where your card details are scanned and cloned your personal data is abstracted and card data like data inside the card is captured and reflashed on a new black card. There are two major types of skimming i.e. physical and digital skimming.

Skimming can be done by adding an Arduino device with an EMV or RFID reader. Always turn your RFID chip off on your debit or credit card since RFID cloning does not require any special tools. An RFID-cloned chip can be reused to make payments.

An EMV chip is a security feature that generates a unique code for each transaction. It can be a hash that is unique and cryptography is used to generate it and hence enhances the security of your card. Every backed credit card like Mastercard or Visa has a unique chip design and standards. The backer has you covered if your card gets hacked. Check the following table shares a lot of information.

Fraud Scenario	Consumer Uses an EMV Card	Merchant has an EMV Point of Sale	Merchant Acquirer is EMV Enabled	Liability is with:
1	No	No	No	Card Issuer
2	No	Yes	Yes	Card Issuer
3	Yes	No	No	Merchant Acquirer
4	Yes	No	Yes	Merchant

IV. WiFi Hacking

Smartphones and all our devices use WiFi and WiFi Hacking is really easy. There are various methods that can be used to hack any WiFi Network. Depending on the standards used, the attacks can vary. There are some common attacks that can be used, WiFi 6 being the most secure WiFi can also be hacked if the device connecting to it is compromised.

ESP8266 for Hacking WiFi

A simple WiFi Jammer can be created and has tons of attack vectors. Becan attack can be used to brute force and disconnect WiFi and connected device. It also has an option to create fake WiFi with the same name thus confusing the user to connect to a WiFi network with the same name and save the password. The Attack can also jam WiFi and work as WiFi jammer thus disconnecting the internet. The packet-dropping technique can force user to disconnect the original wifi. NodeMCU device can be used to craft this kind of attacks and can be powered with a power bank making it compact and undetectable. The device is cheap with price starting from 10$ and available on Amazon.

Image Captured from an actual demonstration of WiFi Hacking by Priyank Gada

V. HID device to Hack Computes including Windows, Linux and OSx

HID device is a device called rubber ducky that uses an ATMEGA32U4 Chip with 4MB of internal memory that can store scripts. This device can be configured to work as a keyboard so even if you have any antivirus, or any policy for security, this device works like a keyboard and can be used to be plugged in any device including a Windows, Linux and even OS X operating system. This device works like a keyboard and can perform any task remotely and operate keyboard including opening shells, running CLI commands and even download and install.

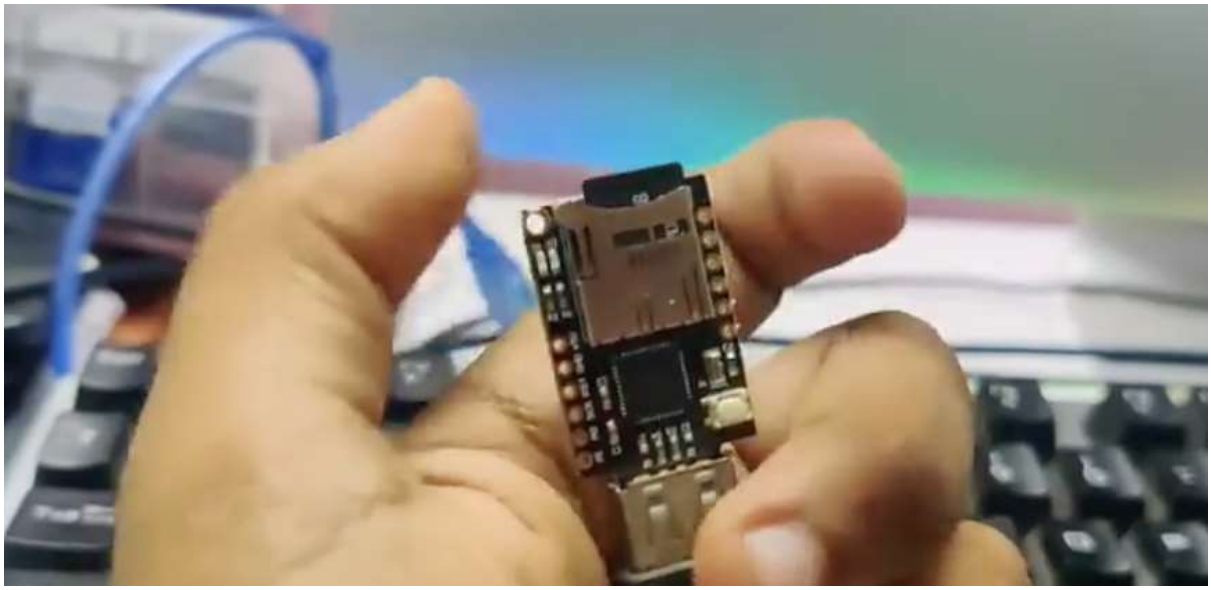
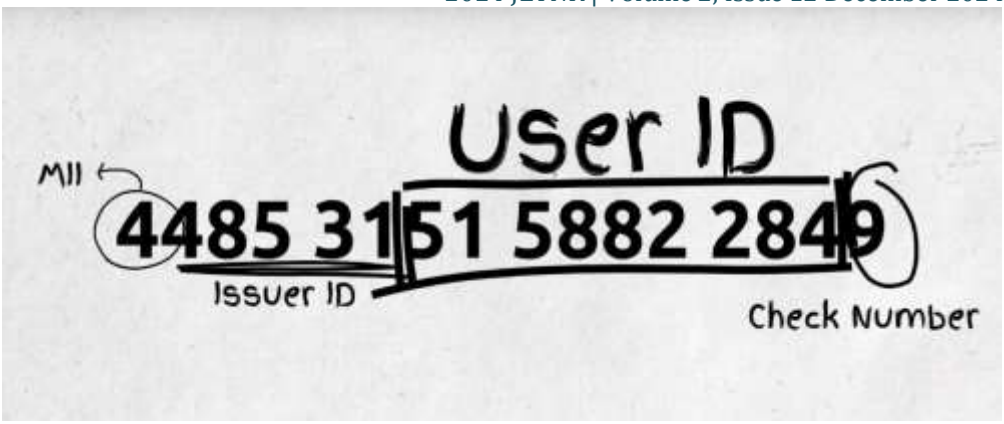


Image is taken from an actual demonstration of Rubber Ducky by Priyank Gada

The device can be configured at home on any windows system and can hold text scripts and python scripts with 4MB file size, that can execute thousands of scripts with just a click of a button. The device is portable and looks like pen drive that can be plugged in any device including Android devices. A size of pendrive does not alert physical security flaws and also works on any device. Device is sold on aliexpress for 10$.

VI. Credit Card Hacking

Credit card hacking is a huge topic discussed among hackers. There are various methods via which a hacker can gain access to credit card details and further use them to make unwanted purchases. A hacker might use keyloggers or create a phishing website that might act as an original website and gather all the required information. The phishing website may look like the original website but hacker has full access to the contents of the website. Credentials like username and password are saved in a simple text files and the user is redirected to the original website with an error message. Whereas key loggers log every key stroke / key presses recorded on the keyboard. This technique requires physical access to the victim's computer. But what if we can generate credit card numbers directly and decrypt the algorithm used by banks to create the cards in the first place. The first digit of any credit card number is the MII . Next 6 digits are is known as the issuer ID . Everything excluding the last digit is the user ID and the last digit is known as the check number.



MII – Major Industry Identifier is the purpose of issuing the credit card. It is a predefined number by the bank and is used to identify the purpose of the card. Following are some MII used by Indian banks. Mostly 4 and 5 number is the first digit used which is issued to the bank.

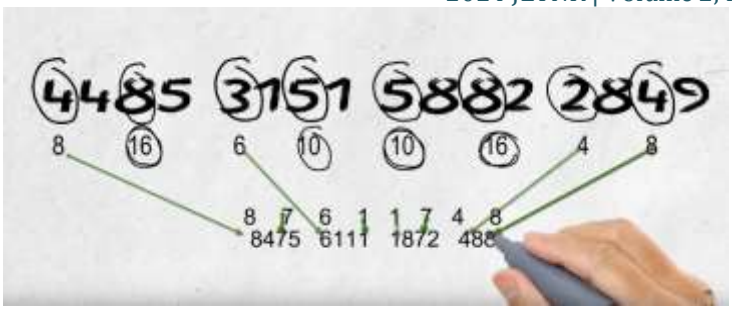
0	ISO / TC and other industry assignments
1	Airlines
2	Airlines and other industry assignments
3	Travel and entertainment
4	Bank and Financial
5	Bank and Financial
6	Merchandising and Banking
7	Petroleum
8	Telecommunication
9	National Assignments.

Issuer ID: Issuer ID is the company which has issued the credit card to the bank. Issuer ID is decided by the company which is backing up the card. Following are some issuer ID's commonly used.

4xxxxx	Visa
34xxxx	American Express
37xxxx	American Express
51xxxx	Master Card
55xxxx	Master Card
6011x	Discover

User ID: User ID is decided by the bank depending on the bank, the branch from where the user has issued the card and the number of cards issued prior in the same branch. This digit are mostly serialized and are not taken seriously.

Luhn Check Algorithm for Credit Cards: Cards issued before 2013 followed the luhn's check algorithm that allowed the bank to check if the card is valid or not. This allows the bank to stop spamming since the algorithm rejects fake and unwanted cards.



Working of Luhn's Check Algorithm : The algorithm checks all alternate numbers from back and doubles them. If the doubled number is 2 digit number then the number is added. All the digits are added up . Added digit should be a multiple of 10.

VII. Call Spoofing

Call Spoofing is a technique where a hacker can flash any number on victim's phone. In other words, a hacker can call from any number and change voice. A hacker might use this technique to call anyone from any number during a social engineering attack. For Eg. A hacker can call a user from a bank number and ask for CVV and other details. This can be done using 2 major methods.

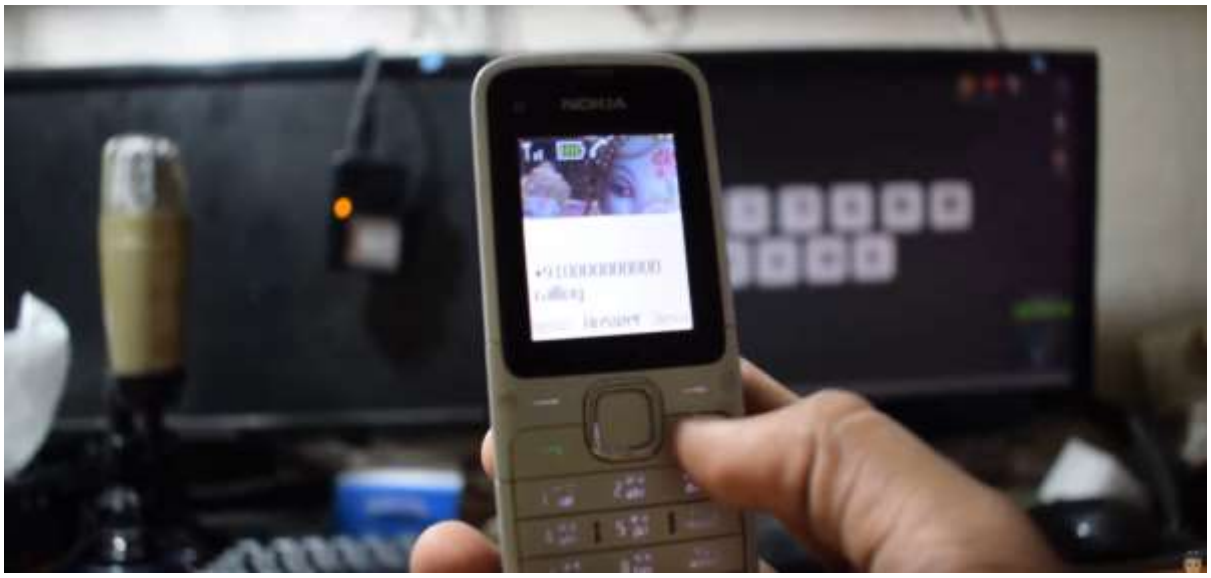


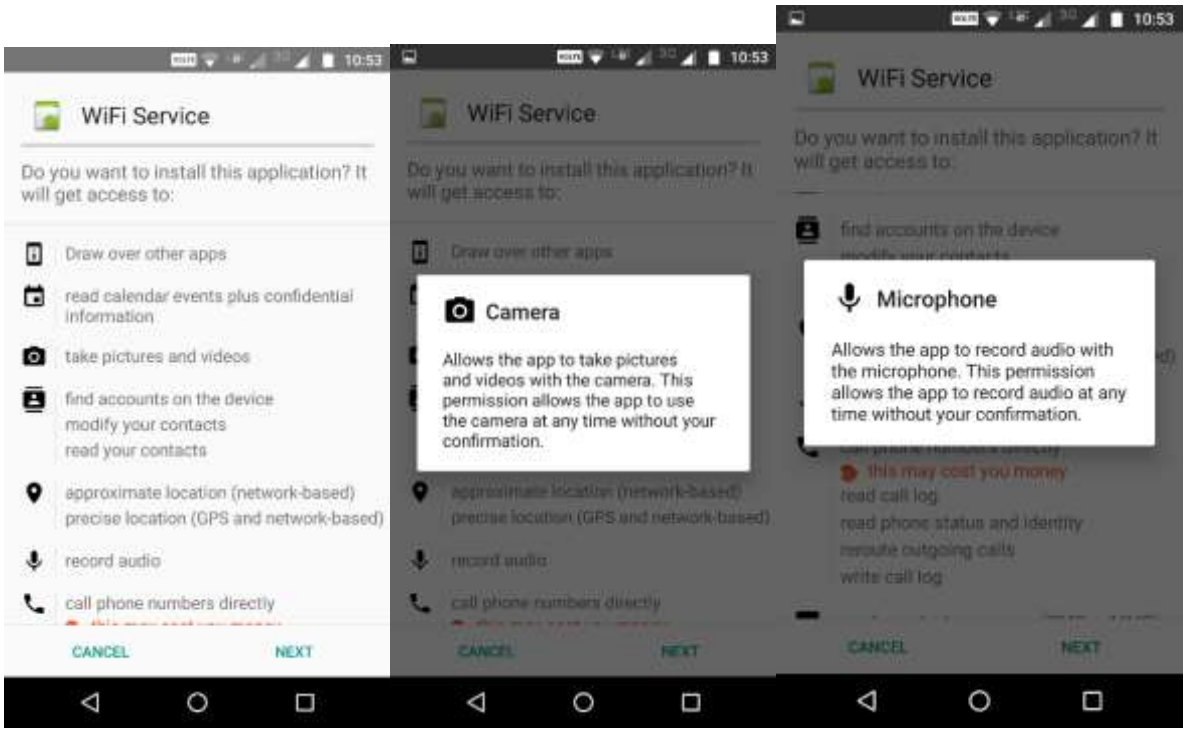
Image taken from an actual demonstration of VoIP call spoofing.

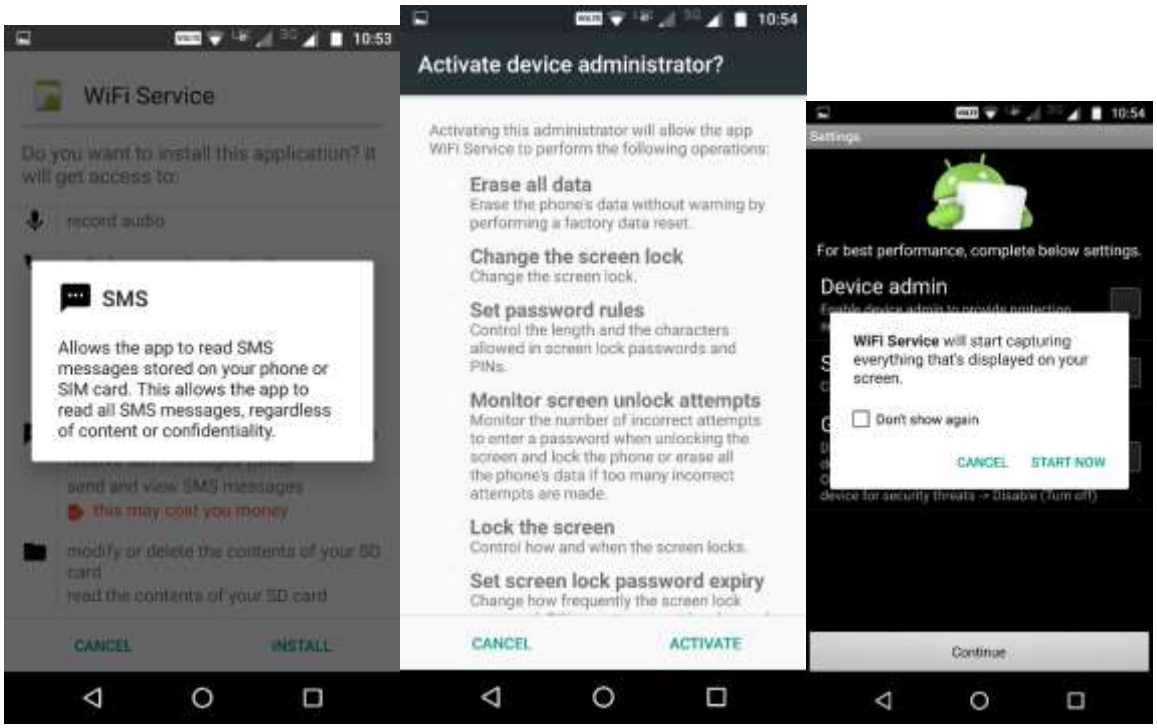
Internet : VOIP calling : VoIP is a technology which allows us to place calls using internet. There are websites that provide VoIP services . The call quality is High definition and clear . Calls placed using VoIP use internet to send packets and thus can be cheap as compared to normal calls. LTE is other technology which uses VoIP and normal calling technique together and converts internet calls into normal call . During this attack a hacker can use servers configured by himself to call from any specified number. There are websites like www.crazycall.net that allow users to call from any specified number .

SNA : Service Number Attack : A service number is a number that is assigned by the service provide . This number routes the call from one user to another and is the intermediate between the calls. If the service number is spammed and bombarded a specific number of times, then the SNS system allows the user to directly call with a specific number. This can help a hacker to place calls from any number.

VIII. Smart Phone Hacking

Smartphones are used on daily basis and hacking a smartphone is not a big thing for a hacker. Android phones use certain API to flash notification in the notification area. This can be accessed by applications to push notifications. Android also allows developers to create application that can request certain permissions to that are required to access modules. If this permission is provided to the applications, then it can **record live audio, live camera and virtually control the smartphone.**





IX. IMEI Numbers and Changing IMEI Numbers.

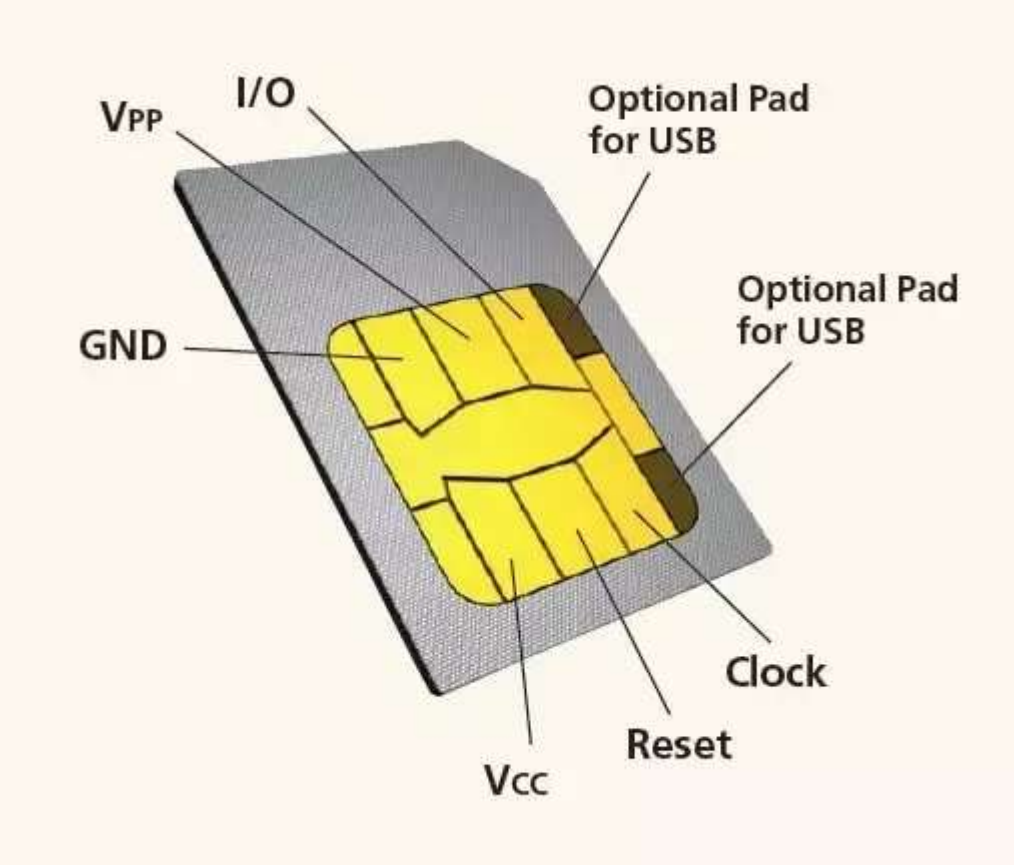
(IMEI stands for International Mobile Equipment Identity Number. IMEI is a unique number given to mobile phones that deal with GSM, UMTS ,and LTE as well as to satellite phones. This number is usually printed behind the battery and is used by cops to track down the phone . The number can be found by

pressing *#06# on the dial pad of the phone. IMEI number is used by a GSM network to identify validity of the device. Once the sim is inserted into the device , IMEI is sent to the service provider. Thus cops use IMEI to find stolen phones. It is easy to change IMEI number , since the number is encrypted into the firmware of the device. MTP and mediatek processors are mostly vulnerable to an attack that allows a hacker to modify firmware of the processors thus a hacker can change IMEI number of any device running on mediatek processor.

A Hacker change the device bootloops and start using meta mode wherein the firmware is installed. Then he / she can use META 3G tool which is specially designed by manufacturers to flash firmware. This tool allows the hacker to change IMEI number of the device including GPS location and other settings. IMEI number and other details are stored in the NVRAM database of the firmware.

X. SIM Cards and SIM cloning

SIM stands for Subscriber identity module . SIM is a integrated circuit that is provided by a service provider that is intended to securely store the IMSI number (international mobile subscriber identity) and a key . This key is used to place calls. SIM also has some storage place wherein the user can store contacts and other details. SIM card contains unique serial number called ICCID , security authentication and ciphering information and temporary information related to network provider and cell towers .



There are 3 basic algorithms used in SIM cards i.e. COMP128v1 , COMP128v2 and COMP128v3 . COMP128 v1 is the first version of algorithm and can be cracked easily and 70% of all the sim cards used today are based on COMP128v1 . COMP128v3 was released in 2013 so SIM cards manufactured after 2013 are not clone-able at least till now.

A hacker can buy a sim card reader and SIM a super SIM to clone any sim card. Super SIM is a AIO sim card that can store upto 15 simcards in one SIM. Magic SIM is a software that can be used to gather information form any sim card and copy and rewrite it to the SuperSIM.

XI. References

[1] Ehacking.net – www.ehacking.net
Learn Ethical Hacking

[2] Priyank Gada – Call Spoofing – Youtube Video
[https://www.youtube.com/watch?v=HrpyBDhl9o4]

[3] Priyank Gada – Change IMEI – Youtube Video
[https://www.youtube.com/watch?v=KIQzQ7QaYRM]

[4] The Magic of Being Hacker – Book
Author – Priyank Gada

[5] Priyank Gada – Credit Card 101 – Youtube Video
[https://www.youtube.com/watch?v=ukIXet5He6w]

[6] Cybrary.it – www.cybrary.it

[7] Sim Clonning – Quora
[https://www.quora.com/How-do-you-clone-a-SIM-card]

[7] Sim Clonning – Youtube Video
[https://www.youtube.com/watch?v=Up1aPiZ-jCk]

[8] Mastercard - Skimming
[https://b2b.mastercard.com/news-and-insights/blog/what-is-skimming-in-cybersecurity/]